CONTENTS AUTHENTICATION SYSTEM AND METHOD, AND RECORDING MEDIUM

Patent number: JP2002024178

Publication date: 2002-01-25

Inventor: IWAMOTO ISAMU

Applicant: WEB I INC

Classification:

- international: ***G06F12/14; G06F12/00; G06F15/00; G06F21/20; G06F21/24; H04L9/32;*** **G06F12/14; G06F12/00; G06F15/00; G06F21/00; G06F21/20; H04L9/32;** (IPC1-7): G06F15/00; G06F12/00; G06F12/14; H04L9/32

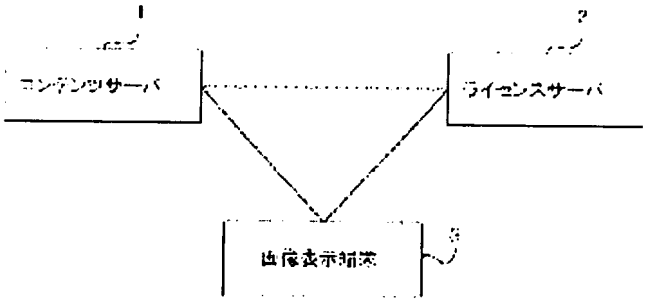
- european:

Application number: JP20000210334 20000711

Priority number(s): JP20000210334 20000711

Abstract of **JP2002024178**

PROBLEM TO BE SOLVED: To provide a contents authentication system or the like for attaining the utilization of contents while preventing disordered duplication and smoothly authenticating the utilization of the contents on the line of low speed/small capacity. SOLUTION: An image display terminal 3 supplies the image ID of an image desired to utilize to a contents server 1 together with its own identification code. The contents server 1 supplies the image data expressing this image to the image display terminal 3 in the state of enciphering the image data with a cryptographic key and transfers the image ID and the identification code of the image display terminal 3 to a license server 2. The license server 2 supplies the cryptographic key for deciphering the image data shown by the transferred image ID to the image display terminal 3 shown by the transferred identification code. The image display terminal 3 acquires the cryptographic key from the license server 2 and stores it in the state of making the specification of contents difficult for a user. Then, the image data are deciphered by this cryptographic key and reproduced in the state of making preservation difficult.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－24178
（P2002－24178A）
(43)公開日　平成14年１月25日(2002.1.25)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ａ　５Ｂ０１７
	12/00	５３７		12/00	５３７Ｈ　５Ｂ０８２
	12/14	３２０		12/14	３２０Ｂ　５Ｂ０８５
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｂ　５Ｊ１０４

審査請求　未請求　請求項の数７　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－210334(P2000－210334)

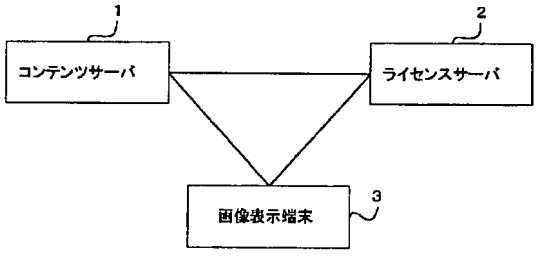
(22)出願日　平成12年７月11日(2000.7.11)

(71)出願人　500327429
株式会社ウェブ　アイ
東京都中野区中央二丁目２番31号
(72)発明者　岩元　勇
東京都中野区中央二丁目２番31号　株式会社ウェブアイ内
(74)代理人　100095407
弁理士　木村　満　（外２名）

Ｆターム(参考)　5B017 AA07 BA07 CA16
5B082 GA11
5B085 AE04 AE29
5J104 AA07 AA13 EA04 JA13 KA02
NA01 NA02 PA10

(54)【発明の名称】　コンテンツ認証システム、コンテンツ認証方法及び記録媒体

(57)【要約】
【課題】　無秩序な複製を防止しながらコンテンツの利用を図り、あるいは低速・低容量の回線でコンテンツ利用の認証を円滑に行うためのコンテンツ認証システム等を提供することである。
【解決手段】　画像表示端末３は、利用したい画像の画像ＩＤを、自己の識別符号と共にコンテンツサーバ１に供給する。コンテンツサーバ１は、この画像を表す画像データを暗号鍵で暗号化された状態で画像表示端末３に供給し、画像ＩＤと画像表示端末３の識別符号とをライセンスサーバ２に転送する。ライセンスサーバ２は、転送された画像ＩＤが示す画像データを復号化するための暗号鍵を、転送された識別符号が示す画像表示端末３へと供給する。画像表示端末３は、ライセンスサーバ２より暗号鍵を取得して、ユーザが内容を特定することが困難な態様で記憶する。そして、この暗号鍵で画像データを復号化し、保存が困難な態様で再生する。



【特許請求の範囲】
【請求項１】端末と、受付サーバと、権限付与サーバとより構成され、
前記端末は、
自己を識別する端末識別情報、及び、利用の許諾を求める対象のコンテンツを特定するコンテンツ識別情報を前記受付サーバに供給する手段と、
ユーザに特定のコンテンツを利用する権限があることを示す権限付与情報を前記権限付与サーバが供給したとき当該権限付与情報を取得し、取得した当該権限付与情報を、操作者がその内容を特定することが困難な態様で記憶する記憶手段と、
前記権限付与情報を用いて復号化可能に暗号化された前記コンテンツを取得し、取得した当該コンテンツを、前記記憶手段が記憶する権限付与情報を用いて復号化して保存が困難な態様で再生する復号化手段と、を備え、
前記受付サーバは、前記端末より前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、前記端末識別情報及び前記コンテンツ識別情報を前記権限付与サーバへと転送する手段を備え、
前記権限付与サーバは、前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、当該コンテンツ識別情報により特定される前記コンテンツを復号化するための前記権限付与情報を、当該端末識別情報が示す前記端末へと供給する手段を備える、
ことを特徴とするコンテンツ認証システム。
【請求項２】前記復号化手段は、前記受付サーバが供給する前記コンテンツを取得する手段を備え、
前記受付サーバは、前記端末より前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、当該コンテンツ識別情報により特定される前記コンテンツを、前記権限付与情報を用いて復号化可能に暗号化された状態で当該端末へと供給する手段を備える、
ことを特徴とする請求項１に記載のコンテンツ認証システム。
【請求項３】前記記憶手段は、前記権限付与情報を暗号化された状態で記憶し、
前記復号化手段は、前記権限付与情報を復号化する手段を備える、
ことを特徴とする請求項１又は２に記載のコンテンツ認証システム。
【請求項４】前記復号化手段は、前記端末が、復号化されたコンテンツを保存する処理を含むプログラムを実行しているか否かを判別し、実行されていると判別したとき、当該プログラムの実行を終了させる手段を備える、
ことを特徴とする請求項１、２又は３に記載のコンテンツ認証システム。
【請求項５】前記端末は、前記コンテンツの対価を決済するための決済用情報を前記権限付与サーバに供給する手段を備え、
前記権限付与サーバは、前記端末より前記決済用情報が供給されたとき、当該決済用情報を取得し、前記権限付与情報を当該端末へと供給する、
ことを特徴とする請求項１乃至４のいずれか１項に記載のコンテンツ認証システム。
【請求項６】端末が、自己を識別する端末識別情報と利用の許諾を求める対象のコンテンツを特定するコンテンツ識別情報とを第１のサーバに供給し、
前記端末が、ユーザに特定のコンテンツを利用する権限があることを示す権限付与情報を前記第１のサーバが供給したとき当該権限付与情報を取得し、取得した当該権限付与情報を、操作者がその内容を特定することが困難な態様で記憶し、
前記端末が、前記権限付与情報を用いて復号化可能に暗号化された前記コンテンツを取得し、取得した当該コンテンツを、前記権限付与情報を用いて復号化して保存が困難な態様で再生し、
前記第１のサーバが、前記端末より前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、前記端末識別情報及び前記コンテンツ識別情報を第２のサーバへと転送し、
前記第２のサーバに、前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、前記第２のサーバが、当該コンテンツ識別情報により特定される前記コンテンツを復号化するための前記権限付与情報を、当該端末識別情報が示す前記端末へと供給する、
ことを特徴とするコンテンツ認証方法。
【請求項７】コンピュータを、
自己を識別する端末識別情報、及び、利用の許諾を求める対象のコンテンツを特定するコンテンツ識別情報を外部に供給する手段と、
ユーザに特定のコンテンツを利用する権限があることを示す権限付与情報が供給されたとき当該権限付与情報を取得し、取得した当該権限付与情報を、操作者がその内容を特定することが困難な態様で記憶する記憶手段と、
前記権限付与情報を用いて復号化可能に暗号化された前記コンテンツを取得し、取得した当該コンテンツを、前記記憶手段が記憶する権限付与情報を用いて復号化して保存が困難な態様で再生する復号化手段と、
して機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コンテンツの不正利用を防止しながらコンテンツを供給するためのコンテンツ認証システム及びコンテンツ認証方法に関する。
【０００２】
【従来の技術】画像データ等のディジタルコンテンツをネットワークを用いて安全に流通させるため、ディジタルコンテンツを暗号化して伝送する手法や、ディジタル

コンテンツのユーザの認証を行う手法が用いられている。

【0003】

【発明が解決しようとする課題】しかし、ディジタルコンテンツは、いったん復号化されたりユーザの認証が行われたりすると、無制限に複製するなどの無秩序な利用が可能であったので、著作権者等ディジタルコンテンツの権利者の利益が損なわれるという問題があった。

【0004】また、暗号化されたディジタルコンテンツをネットワークを介して配信する場合、ネットワークを構成する通信回線の負担が大きくなり、通信速度の低下や、伝送誤りの増加を招いていた。あるいは、十分な通信速度や伝送の正確さを確保するため、通信回線の高速化や大容量化が必要になり、構成が複雑になりしかも通信回線のコストが増大していた。

【0005】この発明は上記実状に鑑みてなされたもので、コンテンツの無秩序な複製を防止しながらそのコンテンツの利用を図るためのコンテンツ認証システム及びコンテンツ認証方法を提供することを目的とする。また、この発明は、低速あるいは低容量の回線を用いてコンテンツの認証を円滑に行うためのコンテンツ認証システム及びコンテンツ認証方法を提供することを目的とする。

【0006】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点にかかるコンテンツ認証システムは、端末と、受付サーバと、権限付与サーバとより構成され、前記端末は、自己を識別する端末識別情報、及び、利用の許諾を求める対象のコンテンツを特定するコンテンツ識別情報を前記受付サーバに供給する手段と、ユーザに特定のコンテンツを利用する権限があることを示す権限付与情報を前記権限付与サーバが供給したとき当該権限付与情報を取得し、取得した当該権限付与情報を、操作者がその内容を特定することが困難な態様で記憶する記憶手段と、前記権限付与情報を用いて復号化可能に暗号化された前記コンテンツを取得し、取得した当該コンテンツを、前記記憶手段が記憶する権限付与情報を用いて復号化して保存が困難な態様で再生する復号化手段と、を備え、前記受付サーバは、前記端末より前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、前記端末識別情報及び前記コンテンツ識別情報を前記権限付与サーバへと転送する手段を備え、前記権限付与サーバは、前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、当該コンテンツ識別情報により特定される前記コンテンツを復号化するための前記権限付与情報を、当該端末識別情報が示す前記端末へと供給する手段を備える、ことを特徴とする。

【0007】この場合、コンテンツは権限付与情報を用いて復号化できる態様で暗号化されて流通され、暗号化されているこのコンテンツは、その利用権限を与えられたユーザの端末により、保存が困難な態様で再生される。従って、このようなコンテンツ認証システムによれば、コンテンツの無秩序な複製を防止しながらそのコンテンツの利用を図ることができる。また、暗号化されたコンテンツ自体は必ずしも受付サーバあるいは権限付与サーバから端末へと伝送されるものではなく、端末、コンテンツ及び利用権限の所在を特定するデータが伝送されればコンテンツ利用の認証という目的は達せられるから、低速あるいは低容量の回線を用いてコンテンツ利用の認証が円滑に行われる。

【0008】前記復号化手段は、前記受付サーバが供給する前記コンテンツを取得する手段を備えてもよい。この場合、前記受付サーバは、前記端末より前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、当該コンテンツ識別情報により特定される前記コンテンツを、前記権限付与情報を用いて復号化可能に暗号化された状態で当該端末へと供給する手段を備えるものであってもよい。

【0009】前記記憶手段は、前記権限付与情報を暗号化された状態で記憶するものとすれば、権限付与情報の漏洩によるコンテンツの不正利用がより確実に防止される。この場合、前記復号化手段は、前記権限付与情報を復号化する手段を備えていればよい。

【0010】前記復号化手段は、前記端末が、復号化されたコンテンツを保存する処理を含むプログラムを実行しているか否かを判別し、実行されていると判別したとき、当該プログラムの実行を終了させる手段を備えることにより、復号化されたコンテンツの保存を阻止する。

【0011】前記端末は、前記コンテンツの対価を決済するための決済用情報を前記権限付与サーバに供給する手段を備えてもよく、前記権限付与サーバは、前記端末より前記決済用情報が供給されたとき、当該決済用情報を取得し、前記権限付与情報を当該端末へと供給するようにしてもよい。これにより、コンテンツ利用の認証を対価を得て行うことが可能となる。

【0012】また、この発明の第２の観点にかかるコンテンツ認証方法は、端末が、自己を識別する端末識別情報と利用の許諾を求める対象のコンテンツを特定するコンテンツ識別情報とを第１のサーバに供給し、前記端末が、ユーザに特定のコンテンツを利用する権限があることを示す権限付与情報を前記第１のサーバが供給したとき当該権限付与情報を取得し、取得した当該権限付与情報を、操作者がその内容を特定することが困難な態様で記憶し、前記端末が、前記権限付与情報を用いて復号化可能に暗号化された前記コンテンツを取得し、取得した当該コンテンツを、前記権限付与情報を用いて復号化して保存が困難な態様で再生し、前記第１のサーバが、前記端末より前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、前記端末識別情報及び前記コンテンツ識別情報を第２のサーバへと転送し、前記第２のサ

ーバに、前記端末識別情報及び前記コンテンツ識別情報が供給されたとき、前記第２のサーバが、当該コンテンツ識別情報により特定される前記コンテンツを復号化するための前記権限付与情報を、当該端末識別情報が示す前記端末へと供給する、ことを特徴とする。

【００１３】この場合、コンテンツは権限付与情報を用いて復号化できる態様で暗号化されて流通され、暗号化されているこのコンテンツは、その利用権限を与えられたユーザの端末により、保存が困難な態様で再生される。従って、このようなコンテンツ認証方法によれば、コンテンツの無秩序な複製を防止しながらそのコンテンツの利用を図ることができる。また、暗号化されたコンテンツ自体は必ずしも第１又は第２のサーバから端末へと伝送されるものではなく、端末、コンテンツ及び利用権限の所在を特定するデータが伝送されればコンテンツ利用の認証という目的は達せられるから、低速あるいは低容量の回線を用いてコンテンツ利用の認証が円滑に行われる。

【００１４】また、この発明の第３の観点にかかるコンピュータ読み取り可能な記録媒体は、コンピュータを、自己を識別する端末識別情報、及び、利用の許諾を求める対象のコンテンツを特定するコンテンツ識別情報を外部に供給する手段と、ユーザに特定のコンテンツを利用する権限があることを示す権限付与情報が供給されたとき当該権限付与情報を取得し、取得した当該権限付与情報を、操作者がその内容を特定することが困難な態様で記憶する記憶手段と、前記権限付与情報を用いて復号化可能に暗号化された前記コンテンツを取得し、取得した当該コンテンツを、前記記憶手段が記憶する権限付与情報を用いて復号化して保存が困難な態様で再生する復号化手段と、して機能させるためのプログラムを記録したことを特徴とする。

【００１５】コンテンツが権限付与情報を用いて復号化できる態様で暗号化されて流通されている場合、暗号化されているこのコンテンツは、ユーザにその利用権限を与えられたとき、上述したような記録媒体に記録されたプログラムを実行するコンピュータにより、保存が困難な態様で再生される。従って、コンテンツの無秩序な複製を防止しながらそのコンテンツの利用を図ることができる。また、暗号化されたコンテンツ自体は必ずしも通信回線を介して伝送されるものである必要はなく、コンピュータには、コンテンツ及び利用権限の所在を特定するデータが伝送されればコンテンツ利用の認証という目的は達せられる。従って、このような記録媒体に記録されたプログラムを実行するコンピュータによれば、低速あるいは低容量の回線を用いてコンテンツ利用の認証が円滑に行われる。

【００１６】

【発明の実施の形態】以下では、この発明の実施の形態にかかるコンテンツ認証システムを、画像ライセンス配信システムを例として説明する。図１は、この発明の実施の形態にかかる画像ライセンス配信システムの構成を示す図である。図示するように、この画像ライセンス配信システムは、コンテンツサーバ１と、ライセンスサーバ２と、画像表示端末３とより構成されている。

【００１７】コンテンツサーバ１及び画像表示端末３は、いずれも、図示しない外部のネットワークに接続されており、コンテンツサーバ１とライセンスサーバ２との間、及び、ライセンスサーバ２と画像表示端末３との間も、このネットワーク等を介して互いに接続される。なお、コンテンツサーバ１、ライセンスサーバ２及び画像表示端末３には、各自に固有の識別符号が割り当てられている。識別符号は、例えば、ＩＰ（Internet Protocol）アドレスより構成されている。

【００１８】コンテンツサーバ１は、図２に示すように、制御部１１と、主記憶部１２と、外部記憶部１３と、送受信部１４とより構成される。主記憶部１２、外部記憶部１３及び送受信部１４は、いずれも内部バスを介して制御部１１に接続されている。

【００１９】制御部１１は、ＣＰＵ（Central Processing Unit）等からなり、外部記憶部１３に記憶されているプログラムに従って、後述する処理を行う。主記憶部１２は、ＲＡＭ（Random Access Memory）等からなり、制御部１１の作業領域として用いられる。

【００２０】外部記憶部１３は、ハードディスク装置等からなり、後述する処理を制御部１１に行わせるためのプログラムを予め記憶する。そして、外部記憶部１３は、制御部１１の指示に従って、自己が記憶するデータを制御部１１に供給する。

【００２１】また、外部記憶部１３は、画像表示端末３に表示させる対象の画像を表す画像データを、暗号化された態様で記憶し、さらに、配信の対象であるこの画像データのＵＲＬ（Uniform Resource Locator）を含んだリンク情報を記憶する。リンク情報は、例えば、配信の対象である画像データＵＲＬと、画像表示端末３のユーザ等がこのＵＲＬが示す画像データを選択するためにマウス等を用いてクリックする対象の画像（バナー）のＵＲＬとを互いに対応付けた形で含むＨＴＭＬ（HyperText Markup Language）文書等から構成される。また、外部記憶部１３は、ライセンスサーバ２に固有に割り当てられた識別符号を記憶する。

【００２２】なお、ＵＲＬは、アクセスする対象のデータを格納するサーバ（例えば、コンテンツサーバ１）と、このサーバが備える記憶装置の記憶領域のうち、アクセスする対象のデータが格納されている記憶領域の論理的位置（ディレクトリ）と、を示す符号である。また、画像データの暗号化は、例えばＤＥＳ（Data Encryption Standard）に準拠した共通鍵暗号の手法により行われている。

【００２３】送受信部１４は、ＤＳＵ（Data Service U

nit）やターミナルアダプタ等からなり、内部バスを介して制御部１１に接続されており、また、上述のネットワークに接続されている。送受信部１４は、制御部１１の指示に従って、制御部１１より供給された情報を、画像表示端末３に宛てて送出する（すなわち、画像表示端末３の識別符号を付してネットワークに送信する）。また、自己宛ての情報（すなわち、コンテンツサーバ１の識別符号が付された情報）をネットワークより受信して、制御部１１に供給する。

【００２４】ライセンスサーバ２は、図３に示すように、制御部２１と、主記憶部２２と、外部記憶部２３と、送受信部２４とより構成される。主記憶部２２、外部記憶部２３及び送受信部２４は、いずれも内部バスを介して制御部２１に接続されている。

【００２５】制御部２１、主記憶部２２、外部記憶部２３及び送受信部２４は、コンテンツサーバ１の制御部１１、主記憶部１２、外部記憶部１３及び送受信部１４と実質的に同一の構成を有している。外部記憶部２３は、後述する処理を制御部２１に行わせるためのプログラムを予め記憶するほか、コンテンツサーバ１が記憶している画像データを識別する画像ＩＤ（IDentification）と、この画像ＩＤにより識別される画像データを復号化するための暗号鍵とを、互いに対応付けて記憶する。

【００２６】画像表示端末３は、図４に示すように、制御部３１と、主記憶部３２と、外部記憶部３３と、送受信部３４と、入力部３５と、表示部３６とより構成される。主記憶部３２、外部記憶部３３、送受信部３４、入力部３５及び表示部３６は、いずれも、内部バスを介して制御部３１に接続されている。

【００２７】制御部３１はＣＰＵ等からなり、外部記憶部３３に記憶されている後述の各プログラムに従って、後述する処理を実行する。主記憶部３２はＲＡＭ等からなり、制御部３１の作業領域として用いられる。外部記憶部３３は、ハードディスク装置等の不揮発性記憶装置からなり、後述する処理を制御部３１に行わせるためのプログラムを予め記憶する。そして、制御部３１の指示に従って、自己が記憶するデータを制御部３１に供給する。

【００２８】外部記憶部３３に記憶されているプログラムには、後述の画像表示プログラムと、後述のブラウザの処理を制御するプログラムとが含まれる。また、外部記憶部３３は、後述する処理により制御部３１が格納する画像データ及び暗号鍵も記憶する。

【００２９】送受信部３４は、モデム、ターミナルアダプタ等からなり、内部バスを介して制御部３１に接続されており、また、ネットワークに接続されている。送受信部３４は、制御部３１の指示に従って、制御部３１より供給された情報を、画像表示端末３に宛てて送出する。また、自己宛ての情報をネットワークより受信して制御部３１に供給する。

【００３０】入力部３５は、キーボード、マウス等より構成されており、操作者の操作に従った情報を、制御部３１に供給する。表示部３６は、ＣＲＴ（陰極線管）、ＬＣＤ（液晶ディスプレイ）等より構成されており、制御部３１の指示に従った画像を、自己が備える表示画面上に表示する。

【００３１】（動作）次に、図１に示す画像ライセンス配信システムの動作を、図５～図８を参照して説明する。図５は、利用権取得時の画像表示端末３の処理を表すフローチャートである。図６は、利用権取得時のコンテンツサーバ１の処理を表すフローチャートである。図７は、利用権取得時のライセンスサーバ２の処理を表すフローチャートである。図８は、画像表示時の画像表示端末３の処理を表すフローチャートである。

【００３２】（利用権取得時の処理）画像表示端末３のユーザがコンテンツサーバ１からの画像の利用権を取得したい場合、ユーザはまず、画像表示端末３の入力部３５を操作して、画像表示端末３に、ブラウザの処理（すなわち、後述のステップＳ１０２及びステップＳ１０３の処理）の実行を指示する（図５、ステップＳ１０１）。

【００３３】画像表示端末３の制御部３１は、ブラウザの処理の実行を指示されると、外部記憶部３３よりブラウザのプログラムデータを読み出し、ブラウザの処理を開始する。ブラウザの処理を開始した制御部３１は、ユーザが、入力部３５を操作して、アクセスする対象のデータのＵＲＬを入力するのを待機する（ステップＳ１０２）。

【００３４】そして、ユーザが、ＵＲＬの入力を完了すると、制御部３１は、入力されたＵＲＬと、画像表示端末３自身に割り当てられている識別符号とを送受信部３４に供給する。送受信部３４は、自己に供給されたＵＲＬ及び画像表示端末３の識別符号を互いに対応付けてネットワークに送信する（ステップＳ１０３）。

【００３５】ステップＳ１０３で送信されたＵＲＬが、配信する対象の画像データのリンク情報が格納されたディレクトリを示している場合、コンテンツサーバ１の送受信部１４は、ステップＳ１０３で送信された情報を受信して制御部１１に供給する（図６、ステップＳ２０１）。制御部１１は、ＵＲＬ及び画像表示端末３の識別符号を供給されると、外部記憶部１３に格納されているデータのうち、送受信部１４から供給されたＵＲＬが示すディレクトリに格納されているリンク情報を読み出す。そして、読み出したリンク情報を、送受信部１４を介し、識別符号が示す画像表示端末３宛てに送信する（ステップＳ２０２）。

【００３６】画像表示端末３の送受信部３４は、ステップＳ２０２で画像表示端末３に宛てて送信されたデータを受信して制御部３１に供給する。制御部３１は、このデータが表すリンク情報を表示することを表示部３６に

指示し、表示部３６は、この指示に従ってリンク情報を表示する（ステップＳ１０４）。リンク情報にバナーのＵＲＬが含まれていれば、制御部３１は、リンク情報に含まれるバナーのＵＲＬが示すディレクトリからバナーの画像データを取得して、表示部３６にバナーの表示を指示する。

【００３７】表示部３６がリンク情報を表示したとき、制御部３１は、ユーザが入力部３５を操作して、配信を受けたい画像データを指定するのを待機する（ステップＳ１０５）。そして、ユーザが画像データを指定すると、制御部３１及び送受信部３４は、ステップＳ１０３の処理と実質的に同一の処理を行うことにより、指定された画像データのＵＲＬ及び画像表示端末３の識別符号を互いに対応付けてネットワークに送信する（ステップＳ１０６）。なお、リンク情報がバナーのＵＲＬを含んでいる場合、ユーザは、例えば、配信を受けたい画像データに対応付けられたバナーを、入力部３５のマウスを操作してクリックすることにより、当該画像データを指定するようにすればよい。

【００３８】コンテンツサーバ１の送受信部１４が、ステップＳ１０６で送信された情報を受信すると、送受信部１４及び制御部１１は、ステップＳ２０１及びＳ２０２の処理と実質的に同一の処理を行う（ステップＳ２０３）。ステップＳ２０３の処理により、コンテンツサーバ１は、ステップＳ１０６で送信されたＵＲＬが示すディレクトリにある暗号化された画像データを画像表示端末３宛てに送信する。画像表示端末３の送受信部３４は、ステップＳ２０３で送信された画像データを受信して制御部３１に供給し、制御部３１は、この画像データを、暗号化されたまま外部記憶部３３に格納する（ステップＳ１０７）。

【００３９】なお、送受信部１４及び制御部１１は、ステップＳ１０３で送信されたＵＲＬが、配信する対象の画像データのＵＲＬである場合は、ステップＳ２０１及びＳ２０２の処理を行うことなく直ちにステップＳ２０３の処理を実行するものとする。

【００４０】また、制御部１１は、外部記憶部１３よりライセンスサーバ２の識別符号を読み出し、画像表示端末３のユーザが指定した画像データ（つまり、ステップＳ１０６で送信されたＵＲＬが示すディレクトリにある画像データ）を示す画像ＩＤ及び画像表示端末３の識別符号を、外部記憶部１３より読み出した識別符号が示すサーバ（すなわち、ライセンスサーバ２）に宛てて、送受信部１４を介し送信する（ステップＳ２０４）。

【００４１】ライセンスサーバ２の送受信部２４は、ステップＳ２０４で送信された、画像表示端末３の識別符号及び画像ＩＤをネットワークを介して受信し（図７、ステップＳ３０１）、制御部２１に供給する。すると、制御部２１は、この画像ＩＤに対応付けられた暗号鍵を外部記憶部２３から読み出し、読み出した暗号鍵と、ステップＳ３０１で受信した画像ＩＤとを、送受信部２４を介し、画像表示端末３に宛てて送信する（ステップＳ３０２）。

【００４２】なお、ステップＳ３０２において、暗号鍵及び画像ＩＤは、外部からの攻撃による決済用データの内容の漏出が防止されるような手順（例えば、ＳＳＬ（Secure Socket Layer）や、ＳＥＴ（Secure Electronic Transaction）や、その他、少なくとも暗号鍵を暗号化して送信するようなプロトコル）に従って送信されることが望ましい。

【００４３】一方、画像表示端末３の送受信部３４は、ステップＳ３０２で画像表示端末３宛てに送信された暗号鍵及び画像ＩＤを受信して制御部３１に供給する（ステップＳ１０８）。制御部３１は、暗号鍵及び画像ＩＤを供給されると、この暗号鍵を後述のステップＳ４０４の処理による復号化が可能な態様で暗号化し、ステップＳ１０７で送受信部３４が受信した画像ＩＤと対応付けて外部記憶部３３に格納する（ステップＳ１０９）。

【００４４】なお、ステップＳ１０９で、暗号鍵及び画像ＩＤは、外部記憶部３３の記憶領域のうち、ユーザが通常参照するデータを格納しないディレクトリに記憶される。こうすることにより、画像表示端末３の操作者の操作により暗号鍵が不正に読み出される事態が防止される。また、暗号鍵は、ステップＳ４０４の処理による以外の手法では復号化が実質的に不可能な態様で暗号化されていることが望ましい。

【００４５】以上説明したステップＳ１０１～Ｓ１０９、ステップＳ２０１～２０４及びＳ３０１～Ｓ３０２の処理により、画像データがコンテンツサーバ１から画像表示端末３へと供給され、ユーザは暗号化された画像データを取得する。また、画像データを復号化するための暗号鍵がライセンスサーバ２から画像表示端末３へと供給され、これにより、画像利用端末３のユーザに画像の利用権が付与される。

【００４６】（画像表示時の処理）ユーザが、暗号化された画像データが表す画像を閲覧するとき、ユーザは、画像表示端末３の入力部３５を操作して、画像利用プログラムの実行を指示する。制御部３１は、この指示に応答して、画像利用プログラムの処理を開始する。

【００４７】すると、制御部３１は、まず、スクリーンショットを作成するプログラム（すなわち、表示部３６に現に表示された画像を表す画像データを作成するプログラム）が実行されているか否かを判別する（図８、ステップＳ４０１）。そして、実行されていなければ処理をステップＳ４０３に進め、実行されていれば、このプログラムの処理を終了させ（ステップＳ４０２）、処理をステップＳ４０３に進める。

【００４８】なお、画像利用プログラムがオペレーティングシステムの制御に従って制御部３１により実行されるプログラムである場合、ステップＳ４０１で制御部３

１は、例えば、オペレーティングシステムが制御しているプログラムを示す情報をオペレーティングシステムの制御に従って取得し、取得した情報に基づき、オペレーティングシステムが、スクリーンショットを作成するプログラムの実行を制御しているか否かを判別するようにすればよい。

【００４９】ステップＳ４０３で、制御部３１は、ユーザが入力部３５を操作して、閲覧を希望する画像の画像ＩＤを入力し、画像閲覧を指示するのを待機する。ユーザが画像ＩＤを入力し、画像閲覧を指示すると、制御部３１は、ユーザが入力した画像ＩＤに対応付けられている暗号化された暗号鍵を、外部記憶部３３より読み出し、復号化する（ステップＳ４０４）。そして、外部記憶部３３に記憶されている暗号化された画像データのうち、ユーザが入力した画像ＩＤにより識別される画像データを、ステップＳ４０４で復号化した暗号鍵を用いて復号化し、復号化した画像データが表す画像を、表示部３６に表示させる（ステップＳ４０５）。なお、復号化された画像データが保存されないようにするため、画像表示端末３は、例えば、画像の表示を終了した後、主記憶部３２や外部記憶部３３に一時的に記憶された画像データがあればこの画像データを消去し、あるいは、外部記憶部３３には復号化された画像データを一時的にも書き込まないようにする。

【００５０】以上説明したステップＳ４０１～Ｓ４０５の処理により、ユーザが利用権を得ている画像データが表す画像が表示される。一方で、この画像のスクリーンショットが作成されるという事態の発生が防止される。

【００５１】なお、この画像ライセンス配信システムの構成は上述のものに限られない。例えば、この画像ライセンス配信システムは、画像表示端末３を複数備えていてもよい。また、コンテンツサーバ１が画像表示端末３に供給する対象のデータは画像を表すデータに限定されず、音声、テキスト、その他任意の情報を表すデータであるいわゆるディジタルコンテンツ全般を含む。

【００５２】また、コンテンツサーバ１は、必ずしもディジタルコンテンツを画像表示端末３に供給する必要はなく、例えば、画像表示端末３のユーザが、予め暗号化されてＣＤ－ＲＯＭ等の記録媒体に記録されたディジタルコンテンツを店頭で入手し、外部記憶部３３にインストールするようにしてもよい。ディジタルコンテンツ利用の認証という目的でネットワークを介して伝送されるデータは、コンテンツサーバ１、ライセンスサーバ２及び画像表示端末３の識別符号や、ディジタルコンテンツのＩＤや、暗号鍵を含んでいれば足りる。従って、ディジタルコンテンツをオフラインで流通させれば、ディジタルコンテンツ利用の認証がより円滑になり、低速あるいは低容量のネットワークでもより容易にディジタルコンテンツ利用の認証という目的が達せられる。

【００５３】また、画像表示端末３は、携帯可能な構成を有し、移動体電話機（例えば、携帯電話や、ＰＨＳ（Personal Handyphone System）や、ＧＳＭ（Grobal Systemfor Mobile communication）など）の端末の機能を行う携帯端末より構成されていてもよい。この場合、送受信部３４は、無線送信機及び無線受信機等を備えるものとし、制御部３１の指示に従って、制御部３１より供給された情報を用いて搬送波を所定の形式で変調し、得られた変調波を送信するものとする。また、送受信部３４は、画像表示端末３宛ての情報を表す変調波（すなわち、画像表示端末３宛の情報を用いて搬送波を所定の形式で変調することにより得られる変調波）を受信して復調し、復調により得られた画像表示端末３宛ての情報を、制御部３１に供給するものとする。そして、この場合、画像表示端末３は、パケット網を介してネットワークに接続されていてもよい。パケット網は、移動体電話通信に用いられる基地局及び電話回線や、この電話回線及びネットワークに接続されたサーバコンピュータ等を備える。パケット網は、画像表示端末３の送受信部３４が送信した変調波を受信して復調し、復調により得られた情報（すなわち、画像表示端末３が搬送波を変調するとき用いた情報）をネットワークに送信するものとする。また、パケット網は、コンテンツサーバ１やライセンスサーバ２から画像表示端末３宛てに送信された情報を受信し、受信した情報を表す変調波を生成して、画像表示端末３に送信するものとする。

【００５４】また、画像表示端末３は、画像利用プログラムの実行中、復号化された画像データを外部のプリンタへと出力することにより、このプリンタに、この画像データが表す画像を印刷させるようにしてもよい。そして、このプリンタが、制御部３１が実行するコマンドに従って画像表示端末３より画像データを取得するものである場合、画像利用プログラムを実行する画像表示端末３は、このコマンドが所定のコマンドであるか否かを判別し、所定のコマンドでないと判別したとき、プリンタへの画像データの供給を中止するようにしてもよい。こうすることにより、不正なプリンタへの画像データの供給を阻止することが可能となる。

【００５５】また、ライセンスサーバ２は、画像表示端末３のユーザが指定した画像を当該ユーザが複製してよい数を表す複製許諾数データを画像表示端末３に供給してもよい。この場合、画像表示端末３の外部記憶部３３は、画像ＩＤと、その画像ＩＤが示す画像の複製許諾数を示す複製許諾数データとを、互いが対応付けられた状態で、ユーザが通常参照するデータを格納しないディレクトリに記憶するようにしてもよい。こうすることにより、画像表示端末３の操作者の操作により複製許諾数データが改竄される事態が防止される。制御部３１等が複製許諾数データを暗号化して外部記憶部３３に格納するようにすれば、複製許諾数データの安全性は更に向上する。そして、画像表示端末３は、画像データが表す画像

が印刷されるなどして複製される毎に、当該画像の複製許諾数を示す複製許諾数データをデクリメントし、複製許諾数データが示す複製許諾数が0以下である画像については、プリンタ等に複製を行わせないものとすればよい。

【0056】また、ライセンスサーバ2は、暗号鍵の送信に先立って画像表示端末3から決済用の情報（例えば、画像を利用する者が決済に用いるクレジットカードのカード番号）が送信されてくるのを待機し、決済用の情報を受信したとき、この決済用の情報を外部記憶部23等に記憶し、画像表示端末3へと暗号鍵を送信するようにしてもよい。

【0057】また、画像表示端末3は、画像データが表す画像を第三者に閲覧させるため、画像データを電子メールに添付して、画像表示プログラムの処理を行う外部の装置へと送信するようにしてもよい。この場合、画像表示プログラムは、例えば、電子メールを受信したこの装置が、受信した電子メールに添付されている画像データについては、複製許諾数が0であるものとしてこの画像データを取り扱うようにこの装置を制御すれば、この装置が画像を不正に複製することが防止される。

【0058】以上、この発明の実施の形態を説明したが、この発明にかかるコンテンツ認証システムは、通常のコンピュータシステムを用いて実現可能である。サーバコンピュータに、上述のコンテンツサーバ1やライセンスサーバ2の動作を実行するためのプログラムを格納した媒体（ROM、フロッピー（登録商標）・ディスク、CD－ROM等）から該プログラムをインストールし、このサーバコンピュータに接続されたパーソナルコンピュータに、上述の画像利用プログラム及びブラウザの処理を制御するプログラムを格納した媒体から該プログラムをインストールすることにより、上述の処理を実行するコンテンツ認証システムを構成することができる。なお、画像利用プログラム及びブラウザの処理を制御するプログラムは、必ずしも同一の媒体に記録されている必要はなく、複数の媒体にこれらのプログラムが分散して記録されていてもよい。

【0059】また、例えば、通信ネットワークの掲示板（BBS）に該プログラムを掲示し、これをネットワークを介して配信してもよい。また、例えば、コンテンツサーバ1が画像利用プログラムを記憶し、画像表示端末3（あるいは画像表示端末3の機能を行うコンピュータ）がネットワークを介してコンテンツサーバ1から画像利用プログラムをダウンロードし、自己にインストールするようにしてもよい。そして、このプログラムを起動し、OSの制御下に、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【0060】

【発明の効果】以上説明したように、この発明によれば、コンテンツの無秩序な複製を防止しながらそのコンテンツの利用を図るためのコンテンツ認証システム及びコンテンツ認証方法が実現される。また、この発明によれば、低速あるいは低容量の回線を用いてコンテンツ利用の認証を円滑に行うためのコンテンツ認証システム及びコンテンツ認証方法が実現される。

【図面の簡単な説明】

【図1】この発明の実施の形態にかかる画像ライセンス配信システムの基本構成を示すブロック図である。

【図2】図1のコンテンツサーバの基本構成を示すブロック図である。

【図3】図1のライセンスサーバの基本構成を示すブロック図である。

【図4】図1の画像表示端末の基本構成を示すブロック図である。

【図5】利用権取得時の画像表示端末の処理を表すフローチャートである。

【図6】利用権取得時のコンテンツサーバの処理を表すフローチャートである。

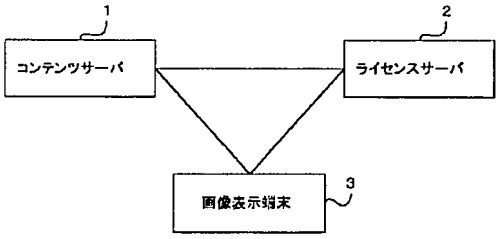
【図7】利用権取得時のライセンスサーバの処理を表すフローチャートである。

【図8】画像表示時の画像表示端末の処理を表すフローチャートである。

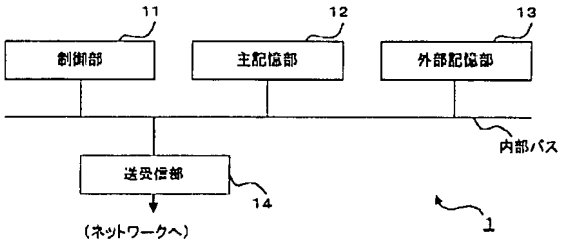
【符号の説明】

1	コンテンツサーバ
2	ライセンスサーバ
3	画像表示端末
11、21、31	制御部
12、22、32	主記憶部
13、23、33	外部記憶部
14、24、34	送受信部
35	入力部
36	表示部

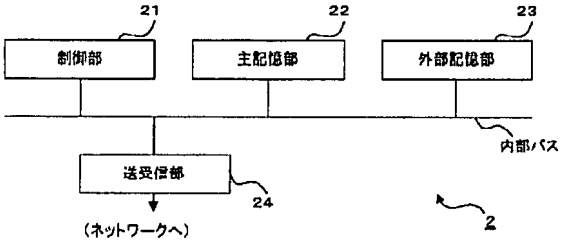
【図1】



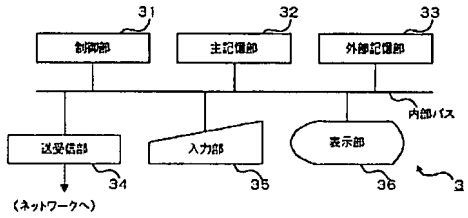
【図2】



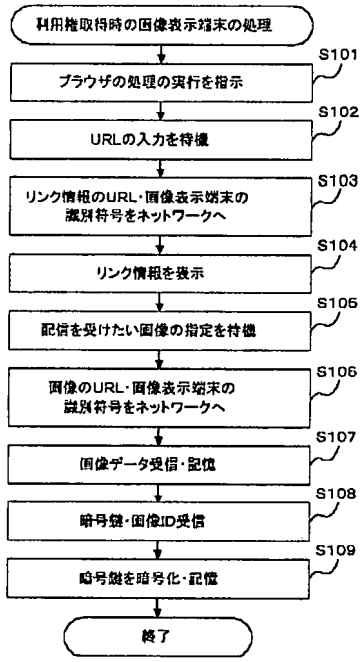
【図3】



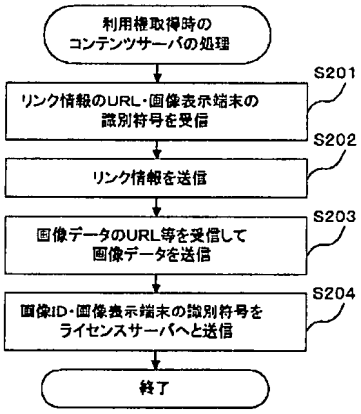
【図4】



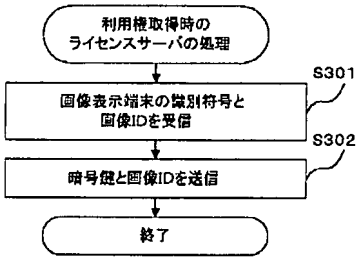
【図5】



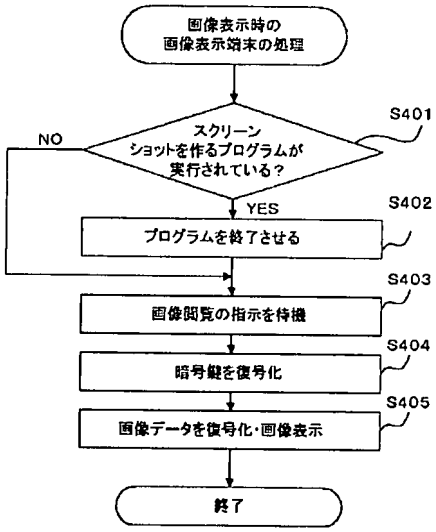
【図6】



【図7】



【図8】


画像表示時の
画像表示端末の処理
S401
スクリーン
ショットを作るプログラムが
実行されている？
NO
YES
S402
プログラムを終了させる
S403
画像閲覧の指示を待機
S404
暗号鍵を復号化
S405
画像データを復号化・画像表示
終了